USFQ LAW REVIEW
Volumen VIII, Núm. 1 • mayo 2021
ISSN: 2631-2573 • ISSN(e): 1390-8014

Las Guerras Cibernéticas en el Derecho Internacional Humanitario: Aplicación de los Principios Rectores del Derecho Internacional Humanitario

Cyber Warfare in International Humanitarian Law: Applicability of the Basic Principles of International Humanitarian Law

María Camila Manotas Valdés*
Irina Burgaentzle Jarrín**

Recibido / Received: 15/01/2020
Aceptado / Accepted: 30/03/2021
DOI: https://doi.org/10.18272/ulr.v8i1.2162

Citación:
Manotas Valdés, M.C., Burgaentzle Jarrín, I. «Las Guerras Cibernéticas en el Derecho Internacional Humanitario: Aplicación de los Principios Rectores del Derecho Internacional Humanitario». *USFQ Law Review, Vol 8, no 1,* mayo de 2021, pp. 71-86, doi: 10.18272/ulr.v8i1.2162

* Universidad San Francisco de Quito USFQ, estudiante del Colegio de Jurisprudencia, casilla postal 17-1200-841, Quito 170901, Pichincha, Ecuador. Correo electrónico: camilamanotas@gmail.com ORCID iD: https://orcid.org/0000-0002-6286-5865

** Universidad San Francisco de Quito USFQ, estudiante del Colegio de Jurisprudencia, casilla postal 17-1200-841, Quito 170901, Pichincha, Ecuador. Correo electrónico: iburgaentzle@gmail.com ORCID iD: https://orcid.org/0000-0001-7880-5296

Resumen

Actualmente, uno de los debates jurídicos se centra en las nuevas tecnologías empleadas para direccionar ataques de origen cibernético, que podrían revolucionar la dinámica utilizada en conflictos armados. A primera vista, varias de estas no cumplirían con principios rectores del Derecho Internacional Humanitario (en adelante DIH), así como los principios de distinción, de proporcionalidad y de precaución. Por lo tanto, este trabajo busca concretar ¿qué desafíos enfrentan los principios del Derecho Internacional Humanitario en las operaciones llevadas a cabo con herramientas ciberespaciales?

Palabras clave

Guerra cibernética, derecho internacional humanitario, principios de distinción, principio de precaución, principio de proporcionalidad.

Abstract

Nowadays, one of the most relevant debates in international law, is about the appearance of new technologies employed in directing cyberattacks. This is essential because it could redirection the dynamic in an armed conflict. On first hand, it would appear that these attacks could not comply with the traditional principles stated in international humanitarian law (IHL), such as the distinction, proportionality and precaution principles. Therefore, this essay seeks to determine what are the challenges that International Humanitarian law face when dealing with cyber tools.

Keywords

Cyber warfare, international humanitarian law, distinction principle, precaution principle, proportionality principle

1. Introducción

La introducción de la tecnología en la sociedad ha demostrado tener un sinnúmero de ventajas, pero a su vez también ha probado tener otra gran cantidad de desventajas. Existen obstáculos que no permiten la adecuada utilización de los medios tecnológicos. Entre ellos se encuentran los hackers al momento de realizar transacciones económicas en línea, publicaciones de pornografía infantil, el *cyberbullying* y los conocidos *trolls* encargados de acosar e intimidar en ciertos escenarios a figuras políticas, principal, pero no únicamente. Sin embargo, la tecnología ha tenido un desarrollo exponencial en varios espacios y plataformas, de tal magnitud que hoy en día se puede hablar de las guerras cibernéticas. La presencia de las guerras cibernéticas es una realidad palpable que los Estados han aceptado como tal, por lo tanto, es imperativo prestar atención a estas guerras, pero sobre todo normarlas para poder regularlas. Es por esto que llevar a cabo una investigación sobre las guerras cibernéticas desde una perspectiva del DIH, en el marco de un conflicto armado internacional (en adelante CAI), se vuelve necesaria. De esta manera se iniciará precisando el concepto de guerra cibernética; cuándo entra en aplicación el DIH y qué regulaciones contiene al respecto. Después, se evaluará si es que los principios del DIH son aplicables en el contexto de una guerra cibernética; y por último se analizará la atribución de responsabilidad de los autores de este tipo de guerras.

2. ¿Qué son las operaciones cibernéticas?

2.1 Denominaciones y definición

Debido al amplio espectro que comprende una plataforma tecnológica, no ha sido tarea fácil llegar a una definición de guerra cibernética que abarque todo lo que este concepto comprende, por parte de los expertos. Melzer ofrece una visión de guerra cibernética que es amparada por lo que establece el DIH. Como expone el citado autor, *cyber warfare* o guerra cibernética se refiere a la guerra realizada en el espacio cibernético a través de los métodos y medios que esta plataforma ofrece. Por ejemplo, la infección o virus que una parte beligerante del conflicto inserta en la red de computadoras de la base militar de su adversario, se constituye como un ataque cibernético[1]. La definición de Melzer trae un primer concepto a colación y es que los actos encaminados a comenzar una guerra cibernética constituyen métodos o medios de guerra del DIH.

1 *Cf.* Traducción libre. Melzer, Nils, *Cyber warfare and international law. Unidir Resources.* (2011): https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Otra forma de definir el presente tema es la propuesta por Eitan Diamond quien dice que el término *cyber warfare* describe las operaciones que son conducidas o relacionadas a un conflicto armado. Estas operaciones involucran el desarrollo y envío de un código de computadora hacia una o más computadoras deseadas, con el objetivo de infiltrarse en su sistema para recolectar, exportar, extraer, destruir, cambiar, introducir nueva información, alterar, desencadenar o manipular procesos controlados por el sistema que fue infiltrado[2]. Diamond expande la idea de guerra cibernética al usar varios verbos rectores, los cuales pretenden arrojar luz sobre los tipos de conducta que pueden constituir un ataque cibernético dentro de la guerra.

Por otra parte, Schaap define las guerras cibernéticas con base en lo dispuesto por el Departamento de Defensa de los Estados Unidos. Esta entidad determina esta modalidad de guerras como el uso de las suficiencias cibernéticas en donde el primer propósito es ejecutar objetivos militares o sus efectos en el ciberespacio o a través de él. También se definen los ataques de redes cibernéticas como las acciones llevadas a cabo mediante el uso de redes computacionales para alterar, restringir, degradar o destruir bien sea la información ubicada en computadoras o redes computacionales o bien la computadora, o la red en sí. Además, el autor postula en su definición de guerras cibernéticas, que dichos ataques sean perpetrados por un Estado en contra de otro[3]. En este sentido, nos estamos refiriendo a un conflicto armado internacional (CAI), ya que las partes son Estados. Vale recalcar que esta investigación se enfocará únicamente en este tipo de escenarios de conflictos armados.

De igual manera es esencial señalar que el Convenio sobre la Ciberdelincuencia celebrado en Budapest, tipifica en sus artículos 2-11 los delitos que pueden darse en esta esfera[4]. Estas normas prescriben delitos tales como acceso ilícito, ataques a la integridad de los datos y del sistema, abuso de los dispositivos, falsificación informática, fraude informático, entre otros. Cabe recalcar que estos delitos han sido descritos de manera amplia para poder enmarcar actos similares dentro del mismo tipo. El esfuerzo realizado por el Convenio sobre la Ciberdelincuencia es otro acercamiento para intentar abordar lo que puede constituir un ataque cibernético y las debidas diligencias que el Estado parte debe realizar.

Adicionalmente, Duggan y Parks mencionan un concepto muy relevante cuando hablamos de esta guerra tan particular. El hecho de que en toda guerra están presentes los ataques y contrataques, o mejor dicho, actos destinados a atacar y actos destinados a defender. Por tanto, no solo existen plataformas,

2 *Cf.* Traducción libre. Diamond, Eitan, *Applying International Humanitarian Law to Cyber Warfare: SSRN.* (Julio 2014): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3093068.

3 *Cf.* Traducción libre. Schaap, Arie. *Cyber Warfare Operations: Development and Use under International Law.* (2009): https://heinonline.org.ezbiblio.usfq.edu.ec/HOL/Page?collection=journals&handle=hein.journals/airfor64&id=123&men_tab=srchresults.

4 Artículos 2-11, Convenio sobre la Ciberdelincuencia, 23 de noviembre de 2001.

virus o softwares con el propósito de ser dañinos, sino que, a su vez, se ha conseguido crear programas que tengan una función exclusivamente protectora[5]. Esto, acompañado con la lectura del artículo 49 del Protocolo Adicional primero a los Convenios de Ginebra[6], podría significar incluso que los softwares que tengan el propósito de defenderse de un ataque, constituyen un acto de violencia, por lo que el DIH entraría en juego.

2.2 ¿Cuáles son los potenciales riesgos que se pueden ocasionar?

En el contexto de un conflicto armado, la guerra cibernética ha sido empleada como una herramienta conjunta. Es utilizada de esta manera porque puede proporcionar diferentes rutas para llegar a un objetivo específico que con los métodos de guerra tradicionales no sería posible. Además, las guerras cibernéticas sí pueden generar daños reales y concretos. Es decir, pueden expresarse no solo en daños en la realidad cibernética, sino también en la realidad material. Así, existirían daños que no siempre pueden ser anticipados por las partes beligerantes, dado su carácter inesperado. Es de suma importancia que el DIH trate tal asunto porque el DIH tiene como objeto brindar el mayor ámbito de protección posible a personas como a bienes, en contextos de conflictos armados. El Comité Internacional de la Cruz Roja (CICR en adelante) en noviembre de 2019, publicó un *position paper* que expone cuáles son sus preocupaciones con respecto a los daños que pueden ocasionarse por un ataque cibernético[7]. El trabajo expone que si bien los ataques están en el entorno de un ciberespacio, las repercusiones pueden expresarse en una realidad tangible, concretamente en infraestructura civil, incluyendo infraestructura sanitaria. Este postulado no resulta descabellado puesto que existe una interconectividad innegable entre las redes computacionales de civiles y militares[8]. Una vez que el virus migra de red a red, es casi imposible retirarlo en vista de que la velocidad a la cual se reproduce resulta incalculable. Al causar una cierta cantidad de réplicas, el virus puede llegar a mutar o convertirse, ya que el receptor puede modificarlo para que cumpla con otro objetivo. En el caso de penetrar en una red o plataforma civil, pueden existir varios escenarios dañosos a la población civil, por ejemplo, ataques a bases de datos para extraer la información del sector financiero, cortar el suministro de agua de hospitales, interferir en la torre de control de un aeropuerto, obstruir la entrega de re-

5 *Cf.* Traducción libre. David Duggan & Raymond Parks, "Principles of Cyber warfare," IEEE Security & Privacy 9, no. 5, (Septiembre 2011): https://ieeexplore.ieee.org/document/6029360.

6 "Artículo 49 - Definición de ataques y ámbito de aplicación

1. Se entiende por ataques los actos de violencia contra el adversario, sean ofensivos o defensivos". Protocolo Adicional I a los Convenios de Ginebra para la Protección de las Víctimas Durante Conflicto Armado, 8 de junio de 1977.

7 *Cf.* Traducción libre. ICRC. *International Humanitarian Law and Cyber Operations during Armed Conflicts. ICRC. (*2019): https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

8 Diamond, *Applying International Humanitarian Law to Cyber Warfare.*

cursos de primera necesidad[9]. Por estas razones, no es correcto decir que los ataques cibernéticos toman lugar en el ciberespacio sin afectar la realidad tangible. Finalmente, los ataques cibernéticos pueden ser utilizados con el fin de generar terror en la sociedad y eso contribuye a debilitar al enemigo. Hay que recordar que el terrorismo es un método prohibido por el DIH, por lo que, si un ciberataque consiste exclusivamente en generar terror a una población, este sería un método de guerra prohibido[10] y constituiría incluso un crimen de guerra. Es así, que no todos los ciberataques pueden ser justificados bajo la regulación del DIH. Teniendo en cuenta lo dicho, se vuelve de suma importancia que los Estados regulen este tipo de ataques, para actuar dentro de tanta incertidumbre. Resulta pertinente revisar algunos ejemplos para evidenciar lo antedicho.

2.3 Casos reales

Se tomarán dos casos calificados como guerras cibernéticas, ocurridos en el marco de un conflicto armado internacional[11], y un tercer caso de ataque cibernético, que, si bien no tiene como contexto un conflicto armado, tiene como propósito ilustrar de manera clara los efectos tangibles de un ataque de este tipo. El primer caso tuvo lugar en Kosovo en 1999[12].

2.3.1. Kosovo 1999

Para comprender el conflicto armado en Kosovo hay que mencionar un antecedente histórico muy importante. Kosovo era una ciudad ubicada en el sur de Serbia cuya población estaba compuesta mayoritariamente por un grupo étnico albanés. Gozaban de mucha autonomía de gobierno hasta que en 1989 el presidente serbio les quitó su autonomía y los puso bajo el régimen de Belgrado, la capital[13]. El conflicto armado comienza en 1998 cuando se enfrentaron militares serbios contra el grupo mayoritario albanés de Kosovo, causando alrededor de 1,500 muertes y la emigración de 400,000 personas. Un año después, el conflicto armado seguía existiendo, por lo que la OTAN planeó una intervención para bombardear Serbia. Se dice que varios grupos de *hackers* pro serbios y anti OTAN como *The Black Hand* intervinieron en el sistema de software de la OTAN para impedir las operaciones que tenía planeado este organismo. Por otro lado, las fuerzas estadounidenses *hackearon* el sistema de las fuerzas aéreas serbias para facilitar un ataque aéreo que se había planeado[14].

9 Diamond, *Applying International Humanitarian Law to Cyber Warfare.*

10 Artículo 51 numeral 2, Protocolo Adicional I a los Convenios de Ginebra para la Protección de las Víctimas Durante Conflicto Armado.

11 Los siguientes casos son todos una traducción libre de inglés a español.

12 *Cf.* Schreier, Fred. *On Cyberwarfare*. DCAF Horizon 2015 Working Paper, No. 7. (2015): https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.

13 NATO (1999). Nato's Role in Kosovo

14 *Cf.* Schreier. *On Cyberwarfare*.

2.3.2. La guerra Rusia – Georgia agosto 2008

Las tensiones entre Georgia y Rusia, dan comienzo en el 2008, dado que un grupo separatista de Osetia del Sur decidió atacar a Georgia[15]. Tras esta intervención, la estrategia militar rusa tomó otro rumbo. En vez de seguir con los tradicionales ataques terrestres, escogieron instaurar una agresiva campaña electrónica contra el gobierno de Georgia. Los objetivos fueron las páginas web estatales, páginas de las instituciones financieras y educativas, incluidas las páginas de las embajadas de los Estados Unidos y de Inglaterra. Por otro lado, el gobierno de Putin decidió atacar a medios de comunicación como la BBC y CNN, por tener información sobre el conflicto muy valorada. Uno de los puntos clave, fue la lesión en la moral nacional de Georgia: fueron incapaces de mantener sus redes informáticas funcionando correctamente, lo que llevó a debilitarse frente a su enemigo. Este caso es muy emblemático ya que fue uno de los primeros donde se pudo evidenciar un manejo exitoso de la tecnología, con sus respectivas ventajas militares. A su vez, se ha convertido en un estándar para poder medir las implicaciones negativas que la cibernética puede traer a la población civil, a pesar de que en este caso no hubo daños tangibles a civiles o a infraestructura tecnológica civil[16].

2.3.3. Ataques cibernéticos contra las instalaciones nucleares de Irán, de 2009 a 2010

En 2009, el presidente Barack Obama, dentro de las tensiones entre Estados Unidos e Irán, decidió continuar con los ataques cibernéticos hacia las instalaciones nucleares en Irán, teniendo como antecedente las tensiones entre las dos naciones[17] las cuales se habían iniciado durante el período anterior con el ex presidente Bush[18]. Los ataques consistían en la infiltración de un *cyber worm* llamado *Stuxnet,* el cual operó en las instalaciones nucleares de Nantanz en Irán (que se encontraba violentando el tratado de no proliferación de armas nucleares de 1970). *Stuxnet* es un arma cuyo objetivo consiste en atacar y deshabilitar los centrífugos nucleares necesarios para la producción de armas. Así, se desaceleró el proceso de creación de armas nucleares de Irán. Stuxnet era capaz de falsificar la información para así camuflarse a través de un control lógico programable[19]. El *cyber worm* era tan efectivo, que era capaz de ocultar el daño causado hasta la etapa final del proceso y recién ahí se manifestaba,

15 *Cf.* White, Sarah. *Understading Cyberwarfare, Lessons from the Russia-Georgia War. Modern War Institute.* (Marzo 2018): https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf

16 *Cf.* Schreier, *On Cyberwarfare*.

17 Es importante recalcar que dichas tensiones no llegaron a calificarse como un CAI.

18 *Cf.* D'Ascanio, Margherita. *Iran victim of Cyberwarfare, ICRC Casebook. ICRC.* (2015): https://casebook.icrc.org/case-study/iran-victim-cyber-warfare.

19 *Cf.* Traducción libre. Lipovsky, Robert. *Seven years after Stuxnet: Industrial systems security once again in the spotlight. We Live Security by Eset.* (Junio 2017): https://www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/.

con lo que se podía registrar el daño. El gobierno iraní confirmó que gran cantidad de su material en proceso de formación resultó dañado y que no sería tarea fácil recuperarse de los perjuicios, estimando un período de meses o años para poder reivindicar el material perjudicado.

Después de revisar estos casos desarrollados en múltiples escenarios, se puede tener una noción más clara acerca de ¿en qué consiste un ataque cibernético? y ¿cómo operan en el contexto de un conflicto armado? Es posible identificar cómo estos ataques podrían representar un riesgo para la población civil en caso de que se asalten plataformas que proveen recursos y suministros esenciales para servicios básicos. Por tanto, es necesario ahondar cómo interactúa el DIH con este nuevo método de conflicto.

2.4 ¿Cuándo entra en juego el DIH en operaciones cibernéticas?

EL DIH interviene en la medida en que una guerra cibernética se lleve a cabo dentro del marco de un conflicto armado internacional o no internacional. El desarrollo de las hostilidades es normado por el DIH:

> La finalidad del Derecho Internacional Humanitario es solucionar los problemas de índole humanitario derivados de los conflictos armados, limitando el derecho de las partes implicadas a elegir los medios y los métodos de hacer la guerra y protegiendo a las personas y a los bienes que pudieran verse afectados por ellos[20].

Sin embargo, los métodos y medios de guerra a los que se hace alusión son los tradicionales. En cambio, los métodos de guerra a los que se refiere esta investigación tienen elementos de otra índole. Como hemos visto, gozan de particularidades tales como el anonimato de quien produce el ataque, el uso de tecnología avanzada, la rapidez y amplitud de la difusión de sus efectos e incluso el hecho de que el ataque pueda ser realizado desde cualquier lugar, lo que significa que las partes no necesitan un contacto directo o cercano. Diamond comenta que en su primera instancia, el DIH no tenía manera de saber cómo evolucionaría la dinámica de un conflicto armado en el futuro, pero el Protocolo Adicional primero a los Convenios de Ginebra, en su artículo 36, confirma que no sería necesario revisar o recodificar los postulados del DIH, porque los Estados tienen la obligación de adecuar cualquier nueva arma o método de guerra a los principios, prohibiciones y normas del DIH[21]:

20 Cruz Roja Española. *Fines y ámbito de aplicación del Derecho Internacional Humanitario. Cruz Roja Española. (Acceso el 29 de noviembre de 2019):* http://www.cruzroja.es/portal/page?_pageid=878,12647065&_dad=portal30&_schema=PORTAL30.

21 *Cf.* Diamond, *Applying International Humanitarian Law to Cyber Warfare.*

> Artículo 36 - Armas nuevas
> Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante[22].

Siguiendo con el argumento de Diamond, él considera que si bien el artículo 36 es un gran paso hacia adelante para poder cubrir el campo de la guerra cibernética y sus implicaciones, existen varios obstáculos cuando se habla de la efectiva aplicación de esta normativa. Como bien menciona Diamond, los hechos deben subsumirse en la ley, de forma que si estos no son del todo claros, difícilmente podría hablarse de una correcta aplicación legal[23]. El autor indica que el acceso a la información necesaria para poder hacer este ejercicio en el caso de las guerras cibernéticas, normalmente se enfrenta a las siguientes dificultades: es poco común que los Estados develen la tecnología que emplean para el desarrollo de sus ataques; la identidad de las partes que conducen los ataques muchas veces es muy difícil de rastrear; y el progreso de las políticas y guías aplicables a las guerras cibernéticas no alcanzan el ritmo al cual estas tecnologías se desarrollan[24].

Por otro lado, cuando las reglas del DIH se queden cortas, es viable aplicar la cláusula *martens*. Dicha cláusula constituye una norma abierta, no precisa qué es exactamente, sin embargo existen varias interpretaciones sobre su alcance y aplicación. Pese a las discrepancias, en la doctrina la interpretación más amplia comprende que cuando la protección no esté regulada por el DIH, se queda protegido por el derecho de gentes o por la costumbre[25]. En este sentido, el vacío normativo que puede dejar una guerra cibernética, puede ser solventado por la cláusula *martens*.

2.5. Normativa supletoria

Subsidiariamente a las reglas del DIH, está el Convenio sobre la ciberdelincuencia, el cual se mencionó previamente. Este fue negociado por el Consejo de Europa con la aclaración de que cualquier Estado fuera de esta región puede formar parte si así lo quisiera. El artículo 39 de dicho convenio estipula que su objeto es "completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes"[26]. Así es como el referido Convenio busca reforzar

22 Artículo 49, Protocolo I Adicional a los Convenios de Ginebra de 1949 Relativos a la Protección de las Víctimas de los Conflictos Armados Internacionales.

23 *Cf.* Diamond, *Applying International Humanitarian Law to Cyber Warfare.*

24 *Cf.* Diamond, *Applying International Humanitarian Law to Cyber Warfare.*

25 *Cf.* Traducción libre. Rupert Ticehurst, "La cláusula de Martens y el derecho de los conflictos armados," *Revista Internacional de la Cruz Roja 22, no. 140* (Abril 1997): p.1, 10.1017/S0250569X00021919.

26 Artículo 39, Convenio sobre la ciberdelincuencia.

Tratados previamente adoptados por los Estados Partes del Consejo de Europa. También busca que los Estados fortifiquen de manera interna su normativa penal, incluyendo las disposiciones relativas a las guerras cibernéticas[27].

Además de las normas que hemos revisado, no se puede dejar de mencionar como una fuente doctrinaria *The Tallin Manual on the Interational Law Applicable to Cyber Warfare.* Este fue preparado por un grupo internacional de expertos por invitación de *The NATO Cooperative Cyber Defence Centre of Excellence (*NATO CCD COE), organización militar con base en Tullin, Estonia, acreditada por la OTAN como un centro de excelencia. En 2009, este centro se reunió con el grupo de expertos con el propósito de juntar en un solo documento la normativa que regula la guerra cibernética. Para poder llevar a cabo este proyecto, se tomaron como modelo otras iniciativas similares, por ejemplo, las realizadas por el Instituto de Derecho Internacional Humanitario, *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*[28]. Este grupo de expertos comenta que este esfuerzo resultó de gran necesidad debido a la relevancia que ha cobrado este distintivo método de guerra desde 1990.

En este sentido es relevante explorar cómo define este instrumento las guerras cibernéticas en el marco de un CAI o CANI. De esta manera, establece que las guerras cibernéticas son ataques hacia computadoras o sistemas computacionales por medio de flujos de datos, lo que constituirá un método de guerra. Es una definición muy parecida a la que ya habíamos mencionado previamente. Adicionalmente, la regla 30 del *Tallin Manual* prescribe que un ataque cibernético es una operación cibernética. Esta puede tener un carácter tanto defensivo como ofensivo, por lo que se espera razonablemente que el ataque cause perjuicio o muerte a personas, o daño y destrucción a objetos[29]. Por lo tanto, se llega a la conclusión de que las definiciones que el *Tallin Manual* aporta son completas. Estas se asemejan a las que se presentaron anteriormente. Lo que busca esta obra doctrinaria es desglosar las guerras cibernéticas en el marco de un conflicto armado con el propósito de analizar cada una de sus aristas por separado, y brindar claridad sobre la información que se tiene sobre cada subtema. Por ejemplo, este cuerpo va desde tener todo un glosario lleno de términos, hasta establecer qué ocurre en un conflicto armado, la responsabilidad de los agentes que producen estos ataques, los daños a las personas y bienes protegidos por el DIH.

Una vez analizada la normativa complementaria al DIH, se vuelve procedente revisar y analizar algunos principios de este derecho.

27 Artículo 39, Convenio sobre la ciberdelincuencia.

28 *Cf.* Traducción libre. International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. *Tallin Manual on the International Law applicable to Cyber Warfare*. Cambridge University Press (2013): http://csef.ru/media/articles/3990/3990.pdf.

29 *Cf.* Traducción libre. International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Tallin Manual on the International Law applicable to Cyber Warfare, art. 30.*

3. ¿Qué principios entran en discusión y por qué?

Aun teniendo lagunas importantes en materia de las guerras cibernéticas, por la falta de regulación en este tema, los principios rectores del DIH toman un rol importante en este aspecto, ya que constituyen directrices en el campo de la cibernética.

3.1 Principio de distinción

No siempre es claro cómo se pueden respetar los principios del DIH, sobre todo unos más que otros, así como el principio de distinción. Este constituye uno de los vectores del DIH, y trata de distinguir tanto entre combatientes y no combatientes, como entre objetivos militares y civiles. De esta forma, se delimita a dónde pueden ser dirigidos los actos de guerra. Bajo este principio se establece que ciertas personas como ciertos bienes, no puedan ser objetivos militares. Los que no participen directamente en las hostilidades, como los que no pertenezcan a una de las partes del conflicto, no pueden ser atacados, así como tampoco pueden serlo los heridos, los prisioneros de guerra o aquellos que hayan dejado las armas. Además, de los civiles, hay otros protegidos por el DIH, como los religiosos y el personal sanitario, así como otras personas que gozan de protecciones especiales[30]. Cumplir con el principio de distinción, requiere de un nivel de direccionamiento muy específico de los ataques por parte de las partes beligerantes. Según Schreier, hay cuatro reglas que se desprenden de este principio. La primera consiste en que los ataques pueden ser solo contra objetivos militares, como consta en el Protocolo Adicional I de los Convenios de Ginebra[31]. La segunda, prohíbe los ataques indiscriminados. En este mismo Protocolo, más específicamente en su artículo 51 numeral cuarto, los ataques indiscriminados son:

> a. los que no están dirigidos contra un objetivo militar concreto;
> b. los que emplean métodos o medios de combate que no pueden dirigirse contra un objetivo militar concreto; o
> c. los que emplean métodos o medios de combate cuyos efectos no sea posible limitar conforme a lo exigido por el presente Protocolo; y que, en consecuencia, en cualquiera de tales casos, pueden alcanzar indistintamente a objetivos militares y a personas civiles o a bienes de carácter civil[32].

30 Artículo 48, Protocolo Adicional I a los Convenios de Ginebra de 1949 Relativos a la Protección de las Víctimas de los Conflictos Armados Internacionales.

31 Protocolo Adicional I a los Convenios de Ginebra de 1949 Relativos a la Protección de las Víctimas de los Conflictos Armados Internacionales.

32 Artículo 51, Protocolo I Adicional a los Convenios de Ginebra de 1949 Relativos a la Protección de las Víctimas de los Conflictos Armados Internacionales.

Continuando con Schreier, la tercera regla versa sobre la necesidad de minimizar los daños colaterales civiles y que estos no sean desproporcionados con respecto a la ventaja militar obtenida. La última, trata sobre la necesidad de tomar las precauciones necesarias para asegurar que lo anterior se cumpla[33]. Ahora, tal como indica Pascucci, la naturaleza misma de los ciberataques no permite que este principio siempre sea satisfecho.

Nos encontramos frente a varios problemas. Uno de ellos es que la protección a civiles no podrá ser siempre la adecuada, puesto que los efectos de un ciberataque pueden llegar a los sistemas civiles, al tener un carácter impredecible e incontrolable[34]. A modo de ilustración, Distein compara un ciberataque con armas biológicas: así como los virus bacteriológicos pueden contagiar no solo a las partes del conflicto sino también a personas protegidas, los virus de computadoras pueden expandirse hasta sistemas civiles. El Comité Internacional de la Cruz Roja, mira con preocupación a los ataques cibernéticos, porque estos podrían no cumplir con el principio de distinción:

> Cuando los ordenadores o las redes de un Estado son objeto de un ataque, una infiltración o un bloqueo, la población civil puede verse privada de servicios básicos como el abastecimiento en agua potable, la asistencia sanitaria y el suministro eléctrico. En caso de paralización de los sistemas de posicionamiento global por satélite (GPS), es posible que haya víctimas civiles, por ejemplo, si se interrumpen las operaciones de vuelo de los helicópteros de rescate que prestan servicios vitales. Las presas, las centrales nucleares y los sistemas de control aéreo también son vulnerables en caso de ataque cibernético, a causa de su dependencia de los ordenadores[35].

El principio de distinción prohíbe también los ataques indiscriminados, es decir, ataques que no apuntan a un objetivo militar específico, concreto. Sin embargo, los ataques a las redes informáticas, sí pueden constituir ataques indiscriminados, dada la interconectividad de las computadoras. Además, el protocolo adicional I, califica de indiscriminado un ataque que trate como un objetivo militar a varios objetivos militares precisos y separados, situados en una zona de habitación civil o bienes civiles[36]. Por lo anterior, es difícil que los ciberataques cumplan con el principio de distinción, pues no siempre están dirigidos contra un objetivo militar concreto, ni tampoco podrían dirigirse contra ellos, puesto que sus efectos no son previsibles y con mayor razón tampoco controlables. De esta manera, se incumplirían los requisitos del artículo

33 *Cf.* Traducción libre. Schreier, *On Cyberwarfare*.

34 *Cf.* Traducción libre. Pascucci, Peter. *Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution. University of Minnesota Law School, Scholarship Repository.* (2017): https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1256&context=mjil.

35 Comité Internacional de la Cruz Roja. *¿Qué límites impone el derecho de la guerra a los ataques cibernéticos? CICR. (Junio 2013):* https://www.icrc.org/es/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

36 *Cf.* Traducción libre. Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts," *Journal of Conflict and Security Law 17, no. 12. (Agosto* 2012), https://doi.org/10.1093/jcsl/krs016.

51 ya citado, que establece los ataques que son considerados indiscriminados. Como hemos visto, el principio de distinción no siempre puede ser satisfecho en las guerras cibernéticas, por lo que el daño colateral que se da en civiles, existe.

3.2 Principio de proporcionalidad

Con esto último, entra en juego el principio de proporcionalidad. Este principio dispone que los daños colaterales a civiles que resulten de algún ataque dentro del marco de un conflicto armado, no pueden ser excesivos en comparación con la ventaja militar directa y concreta que se pueda obtener del ataque, es decir, la ventaja militar debe ser superior a los daños incidentales. Como apunta Dinstein, el principio de proporcionalidad descansa en la previsión del daño colateral y en la expectativa de la ventaja militar, es decir, concluye en la obligación de un análisis previo al ataque. En el caso de que un ataque produzca daños excesivos inesperados e imprevistos, el ataque no sería considerado como una violación al principio de proporcionalidad. Además, la ventaja militar debe ser concreta y directa, y –siguiendo con Dinstein– esto significa que se debe evaluar cada uno de los elementos, por más aislados que sean, con respecto a la ventaja militar. En la cibernética el ataque se da en contra de una serie de computadoras, pero solo tomando a todas las computadoras como un conjunto, se podría realmente identificar la ventaja que esto traería[37].

Por otro lado, Pascucci trae a colación el problema de definir los efectos indirectos o bien los efectos rebote que puede traer consigo una guerra cibernética. Este tipo de efectos se da debido a la interconectividad de las computadoras y de los sistemas en el ciberespacio. Citando el Manual de Tallin, este autor dictamina que estos efectos indirectos comprenden las consecuencias demoradas o desplazadas de la acción. No obstante, no resulta claro cuantos niveles de este efecto cascada deberían ser tomados en cuenta como daño colateral para así proceder con el análisis de proporcionalidad. No solo eso, sino que tampoco es evidente el nivel de detalle y precisión necesarios para determinar estos rubros. Por otra parte, es importante anotar que los datos que guardan las computadoras pueden variar tremendamente en cuestión de minutos, por lo que prever cuál sería el daño colateral causado a un determinado sistema cibernético, no siempre puede ser acertado. Es decir, si un ataque dentro de un conflicto es planeado en contra de cierto objetivo militar, muy probablemente, a la hora que efectivamente se de dicho ataque, el objetivo militar podría haber cambiado drásticamente. Es por esto que el análisis de un daño colateral excesivo se vuelve proporcionalmente más complejo[38]. Si bien es cierto que

37 *Cf.* Traducción libre. Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts.*
38 *Cf.* Traducción libre. Pascucci, *Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution.*

los objetivos militares tradicionales también son cambiantes, la magnitud y la rapidez con la que pueden cambiar los objetivos cibernéticos es la que marca una diferencia significativa entre unos y otros.

3.3. ¿Participación directa?

Se analizará primero qué acciones consisten en participación directa y cuáles no. Aquí nos preguntamos: ¿construir un *malware* constituye una participación directa? La importancia de discutir esto reside en que los civiles que participen directamente en las hostilidades se convierten en objetivos militares, por lo tanto, pueden ser atacados y pierden su protección, como consta en el Protocolo Adicional I[39] .

Melzer, a través de ciertos estándares, nos aclara qué actos implican una participación directa de los civiles en las hostilidades. La participación directa tiene como base tres estándares, que son: el umbral de daño; la causalidad directa, y por último el nexo beligerante. Para que se considere como directa una participación, debe haber dentro del umbral de daño, probabilidades de que el acto tenga efectos adversos en las operaciones militares o sobre la capacidad militar de la parte adversa, o bien, que cause muertes, heridas o destrucción de personas o bienes protegidos contra los ataques directos. Analizando la causalidad directa, Melzer establece que debe existir un vínculo causal directo entre el acto y el daño. Por último, sobre el nexo beligerante, se busca que el propósito específico del acto cause directamente el umbral de daño exigido[40]. Hay otros autores, como Rodríguez-Villasante, citado por Reguera, que opinan que la participación tiene que ver con la preparación del ataque, desde que comienza hasta que termina la participación activa. Reguera, en cuanto a los ciberataques, afirma lo siguiente:

> De la misma manera puede ocurrir con los ciberataques. Así, por ejemplo, un hacker podría preparar un virus para ser introducido en el sistema informático que controla los procesos de una planta de depuración de aguas y que, al cabo de unos días, provoque muertos por envenenamiento entre la población. El inicio de la participación directa lo definiría el momento en que empieza a diseñar el virus informático, sin embargo el final no queda claro. Se podría decir que acaba cuando lanza el virus, aunque los efectos se manifiesten después. Cabe también preguntarse si se le podría atacar, en el momento de conocer los efectos, aunque haya pasado ya un tiempo[41] .

39 Artículo 51, numeral 3, Protocolo I adicional a los Convenios de Ginebra de 1949 Relativos a la Protección de las Víctimas de los Conflictos Armados Internacionales.

40 *Cf.* Melzer, Nils. *Guía para Interpretar la Noción de Participación Directa en las Hostilidades según el Derecho Internacional Humanitario*. CICR. (Diciembre 2010): https://www.icrc.org/es/publication/guia-participacion-directa-hostilidades-derecho-internacional-humanitario-dih.

41 Reguera, Jesús. *Aspectos legales en el ciberespacio. La ciberguerra y el derecho internacional humanitario. GESI.* (Marzo 2015): http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario.

Reguera, basándose en Rodríguez-Villasante, opina que la participación directa dentro de una guerra cibernética ocurre desde el momento de la preparación hasta cuando se termina el acto. Sin embargo, sigue la duda de si toda preparación debería contarse como una participación directa. Finalmente, el *Tallin Manual*, nos da una dirección más clara. En la regla 35, sobre la participación directa en las hostilidades por los civiles, numeral 4, se toman los tres criterios de Melzer para calificar la participación e incluye un ejemplo: en cuanto al umbral de daño, habría una participación directa en caso de un ciberataque que interrumpa las órdenes del enemigo y el control de su red. En la causalidad directa, hablaríamos de que la interrupción de las órdenes del enemigo como el control de su red, hayan sido causa directa de dicho ataque. Se cumpliría con el nexo beligerante si es que el sistema fue utilizado para dirigir las operaciones militares. También se advierte, dentro del Manual, que existieron diferencias de opiniones en cuanto a la aplicación de los criterios para acciones muy particulares[42].

4. ¿Cómo se atribuye la responsabilidad en ataques cibernéticos?

4.1 Anonimato

Hablar de responsabilidad en el marco de guerras cibernéticas, no resulta una labor fácil de determinar, pues es bien sabido que una de las características del espacio cibernético, es el anonimato. Efectivamente, exigir responsabilidades no siempre es posible dado que los actores en el mundo electrónico pueden no ser identificables, pueden ser varios y no todos se encuentran en un mismo lugar. Esto hace que imputar responsabilidad sea una tarea complicada. Identificar la fuente o servidor en donde se originó un ciberataque, es dificultoso. Además, pasar de ahí a identificar los autores reales de dicho ataque, es aún más complejo, pues no siempre el responsable del ciberataque será el que está detrás de dicho servidor. También, en el caso de que se lograra rastrear una dirección IP u obtener algún indicio que lleve a alguna posible identidad, esta no siempre podría dar con el autor material. Esto último, por el hecho de que los dispositivos mutan con una rapidez y una facilidad exponencial que pueden dirigir la búsqueda a un sinfín de ubicaciones, ya que el hecho de rastrear los servidores puede ser también *hackeado*. Otra de las complicaciones es el llamado “ordenador zombi”, mediante el cual una tercera persona tiene el manejo de otro ordenador, sin que el dueño del ordenador tenga conocimiento de lo sucedido[43]. El resultado de esto es que muchas veces se deja en la im-

42 *Cf.* Traducción libre. International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual on the International Law applicable to Cyber Warfare*.

43 *Cf.* Reguera, *Aspectos legales en el ciberespacio. La ciberguerra y el derecho internacional humanitario.*

punidad las violaciones al derecho internacional humanitario ocurridas en el campo cibernético. Ahora, si es que la normativa llegara al nivel de desarrollo en el que no sea posible la impunidad, probablemente las partes beligerantes harían todo lo posible y necesario para cumplir con la normativa y principios analizados con anterioridad.

5. Conclusión

Para concluir, las guerras cibernéticas se desarrollan en el ciberespacio, lo que podría para algunos llegar a ser un concepto abstracto. Sin embargo, las guerras cibernéticas sí pueden llegar a tener repercusiones en la realidad tangible. De hecho, la historia nos muestra que esto efectivamente ocurre, ocasionando graves daños materiales. Vale la pena mencionar que estos ataques resultan relevantes para el DIH siempre que se den en el marco de un conflicto armado. No obstante, la regulación de las guerras cibernéticas resulta un desafío puesto que la rapidez con la que se desarrollan los medios tecnológicos es exponencial frente al paso con el que las regulaciones pueden ser modificadas y más que nada adecuadas a las nuevas realidades. Por esta misma razón, la aplicación de los principios del Derecho Internacional Humanitario en las guerras cibernéticas se convierte en un reto. Este es un tema que sin duda es relevante, no está completamente explotado y existen muchas aristas por analizar. Además, esta investigación debe ser hecha por los Estados en conjunto con especialistas de la cibernética. Sin duda, se necesitan soluciones para encontrar mecanismos de aplicación en esta modalidad de guerras, para que estos puedan cumplir con el objetivo del derecho internacional humanitario, que es dar el mayor ámbito de protección posible a los civiles y en general a aquellas personas y objetos protegidos por este derecho.